

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION**

UNITED STATES OF AMERICA

Case No. 1:18-CR-0043

Judge Timothy S. Black

v.

**YANJUN XU
(a/k/a Xu Yanjun and Qu Hui)**

**UNITED STATES' MOTION
IN OPPOSITION TO DEFENDANT'S
MOTION FOR JUDGMENT OF
ACQUITTAL**

Comes now the United States of America, by and through Assistant United States Attorneys Timothy Mangan and Emily Glatfelter and Trial Attorney Matthew McKenzie, respectfully submitting this Response in Opposition to the defendant's Motion for Judgment of Acquittal for the Court's consideration. For the reasons stated below, the defendant's motion is meritless and should be denied.

The Court Should Deny Defendant Xu's Motion for Acquittal

Federal Rule of Criminal Procedure permits a defendant to move for a judgement of acquittal after the government closes its evidence, and provides that a court must enter such judgment as to any offense for which the evidence is insufficient to support a conviction. F.R.C.P. 29(a). The test for determining sufficiency of the evidence is "whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia*, 443 U.S. 307, 319 (1979). "In addressing a Rule 29 motion, the Court may not make credibility determinations, and may not weigh the evidence." *United States v. Salaam*, 2021 WL 2217066 at 1* (S.D. Ohio 2021) (quoting *United States v. Gen. Elec. Co.*, 869 F. Supp. 1285, 1290 (S.D. Ohio 1994) (citing

United States v. Davis, 981 F.2d 906, 908 (6th Cir. 1992)). It is well established that “a defendant claiming insufficiency of the evidence bears a very heavy burden.” *United States v. Graham*, 622 F.3d 445, 448 (6th Cir. 2010). And, ““circumstantial evidence alone can defeat a sufficiency challenge.”” *United States v. Brooks*, 987 F.3d 593, 603 (6th Cir. 2021) (quoting *United States v. Maya*, 966 F.3d 493, 500 (6th Cir. 2020)).

The defendant essentially offers two arguments as to why his motion for an acquittal should be granted: 1) there is no evidence that he joined a conspiracy to steal trade secrets with respect to Counts One and Two; and 2) there is no evidence that he intended to steal trade secrets with respect to Counts Three and Four. Both arguments fail under the weight of the evidence produced at trial, particularly when viewed in the light most favorable to the government. As a result, defendant’s motion should be denied.

1. There is ample evidence that the defendant conspired with others to steal trade secrets.

Count One alleges that the defendant conspired to commit economic espionage in violation of 18 U.S.C. § 1831, and Count Two alleges that the defendant conspired to commit trade secret theft in violation of 18 U.S.C. § 1832. It is well-established that to prove a conspiracy the government need not present direct evidence of an agreement. *See, e.g., United States v. Thompson*, 533 F.2d 1006, 1009 (6th Cir. 1976). An agreement “may be inferred from circumstantial evidence that can reasonably be interpreted as participation in a common plan,” *United States v. Ellzey*, 874 F.2d 324 at 328 (6th Cir. 1989) or “from acts done with a common purpose.” *United States v. Frost*, 914 F.2d 756, 762 (6th Cir. 1990).

The defendant contends that no rational juror could find the defendant joined a conspiracy to steal information the conspirators believed to be a trade secret. However, the record simply belies the defendant’s contention. Relevant here, “trade secret” is simply technical or engineering

information, designs, techniques, or processes that “the owner thereof has taken reasonable measures to keep such information secret” and “the information derives independent economic value” from not being generally known. 18 U.S.C. § 1839(3). The record is replete with evidence that the defendant agreed with others to illicitly acquire such information.

Over the past two weeks, the government has presented substantial evidence from which a juror could conclude that the defendant knowingly joined a conspiracy to commit economic espionage and commit theft of trade secrets. First, the government provided a framework, through the testimony of Dr. Mulvenon, of how the PRC Government functions and that it tasks its primary intelligence agency, the Ministry of State Security (MSS), with illicitly acquiring foreign technology. Mulvenon explained how the Ministry of Industry and Information Technology works with various state owned enterprises (SOEs) to identify gaps in PRC technology. The MSS—particularly the 6th Bureau of the MSS and its regional affiliates such as the JSSD—then works with experts from the SOEs to identify and obtain the missing information and provides it to the SOEs. Through the testimony of Rizwan Ramakwadala, the jury learned that the Chinese government, via its SOEs, has been trying to manufacture a gas turbine engine with composite fan blade technology – the same one manufactured by GE Aviation – for years. The government then produced evidence of what amounted to a case study in PRC economic espionage to obtain aviation technology.

Specifically, the government produced evidence of the defendant and individuals, such as Chai Meng and Xu Heng – who any rational juror could conclude to be fellow members of the MSS/JSSD – engaging in communication and taking actions against aviation companies between approximately 2013 and 2018 that demonstrated their conspiratorial objective. For example, the government presented evidence that in approximately 2014, the defendant his MSS colleagues first

hacked the French aviation company Safran, using company insiders that they had recruited.¹ Special Agent Adam James testified that he analyzed the Safran-issued hard drive that Mr. Hascoet took to China in January 2014. James confirmed that malware was installed on the hard drive on January 15, 2014 – a date which coincided with messages between the defendant and the assets he had recruited inside the company discussing the “planting” of a “horse.” From the communications between the defendant, the company insiders, and the defendant’s MSS colleagues, such as Chai Meng, a rational juror could conclude that the internet intrusion was conducted by the defendant and his colleagues for the benefit of China. (*E.g.* Gov. Ex. 110, p. 6 (“Do they think China is hacking them?”).) Moreover, a juror could conclude from the communications paired with the testimony of Mr. Hascoet – the Safran employee whose computer was infected with malware when he visited a plant assembling LEAP engine parts – that the defendant and his colleagues were conspiring to obtain secret technology about the LEAP engine. Conducting an internet intrusion against Safran is consistent with designing an intelligence operation to obtain information that is not publicly available. The defendant’s conduct in managing human sources inside Safran, along with his communications with MSS colleagues speaks volumes about the conspiratorial agreement that he knowingly joined.

The government also presented evidence that approximately a year after the Safran hacking, the defendant, posing as “Qu Hui,” attempted to recruit a Boeing IT project manager for an exchange about network security. (Gov. Ex. 92.) The Boeing IT manager explained how, prior to becoming a project manager, he had been responsible for data retention, meaning all of the design, testing and flight data related to individual Boeing aircrafts. The defendant aggressively pursued the Boeing IT manager, even after the Boeing manager explained that network security

¹ The evidence at trial demonstrated that Safran has a joint venture with GE Aviation to produce the LEAP engine, which contains a composite fan blade and containment system.

was not his expertise. The Boeing manager finally agreed to meet with “Qu Hui” and two colleagues, one of which was “Chai” when he returned to China to visit family. They met in a hotel lobby for 15-30 minutes, after which Qu Hui insisted on reimbursing the Boeing IT manager’s travel expenses. When the Boeing IT manager declined reimbursement, which he viewed as unethical, Qu Hui contacted him more than five times about payment, even referencing that he had contacted the manager’s father. *Id.*

The government also presented evidence that in 2017, the defendant and his MSS colleagues invited Arthur Gau for a presentation in a hotel room in China with three engineers. The jury heard evidence that Gau worked as an engineer for Honeywell and Honeywell is a U.S.-based company that manufactures engines components. Gau testified that along with Xu, Chai Meng was present for the meeting. The defendant paid Gau \$10,000 for the presentation -- \$5000 the year before and \$5000 after the presentation, in addition to the airfare. After Gao left the room, a transcript captures the defendant and his conspirators discussing options for recruiting and using Gau in the future. (Gov. Ex. 86c.) During the meeting, the defendant acknowledges that using insiders to take “large batches of information” might be difficult because the “security” is tight at those companies. (*Id.* at 4-5.) After the meeting, Xu called Chai Meng and chided him for using an alias with Gau that did not make sense. (Gov. Ex. 86d.)

The government presented other evidence regarding the communications and tactics of the defendant and his MSS colleagues in using tradecraft to acquire foreign aviation technology. For example, the government presented evidence of instructions that the defendant had received from his conspirators on the specific types of technological information to obtain (*E.g.* Gov. Ex. 43(e) (conversation regarding which Boeing documents to obtain); Gov. Ex. 6e (list of collection requirements recovered from Belgium phone); Gov. Ex. 69 (list of “domestic requirements”); and

Gov. Ex. 89 (Gau tasking list from 2017), and then saw evidence or heard testimony that the defendant tried to obtain such information from the employees of foreign aviation companies. Based on the defendant's deception in using aliases with these employees, the evidence surrounding the defendant's meetings with these foreign employees, and the defendant's cash payments to these employees in exchange for the information, the jury could infer that the defendant was seeking non-public foreign technology that the defendant otherwise could not obtain.

Additionally, the combination of WeChat communications and the defendant's calendar entries, showed clandestine tactics employed by the defendant and his MSS colleagues against aviation engineers visiting China. Specifically, a section of MSS would steal information from the electronic devices of visiting engineers while such engineers were being entertained away from their hotel rooms. (Gov. Exs. 44a and 45a.) The jury also saw communications between the defendant and engineers at AVIC using codes to discuss foreign aviation technology (Gov. Exs. 41b and 42b); the defendant instructing conspirators to only let the targets of his tradecraft know his alias and cover job (Gov. Ex. 43e ("The guest doesn't know our identity. I've approached him with the name of Hui Qu, the Deputy Secretary-General of the Science and Technology Association")); evidence that the defendant represented himself as working for two cover organizations – a provincial Science and Technology Association and Nanjing Loute (*id*; Gov. Ex. 11c (French visa records); *see also* Gov. Ex. 56b (dossier providing fictitious positions and background of Nanjing Loute)); and a conspicuous *lack* of evidence indicating that the defendant worked for either cover organization – particularly in comparison to substantial records indicating that the defendant was actually a Deputy Directory in the MSS (Gov. Ex. 21b (cadre application).

With respect to GE Aviation, the government presented, among other things, emails about collections requirements (Gov. Ex. 69) and a tasking sheet (Gov. Ex. 6e), which Nick Kray, a senior GE Aviation engineer who has worked on composite technology for thirty years, testified contained terms about composite fan blade and containment systems – one of the key technologies that GE Aviation seeks to protect from disclosure. And, Eric Ritter, GE Aviation’s Vice President of Cyber Security, explained that GE Aviation takes substantial measures to protect key technologies, and described how the type of file directory requested by the defendant, revealed significant information about GE Aviation files and how it would be beneficial for those posing an external threat to the company. Additionally, the government introduced evidence in the form of testimony, recordings, emails, and messages regarding the defendant’s attempts to meet Employee 1 under false pretenses in Belgium and to induce GE Employee 1 to bring a hard drive containing the contents of his GE Aviation work computer — which the jury could infer the defendant had every reason to believe contained trade secrets after seeing a directory of the contents of said computer approximately a month earlier. Moreover, based on communications with Employee 1, the defendant knew that GE Aviation took steps to protect this electronic data from disclosure. (Gov. Exs. 67-77)

The defendant did not act alone on his mission to obtain these trade secrets in Belgium, and the circumstances of his arrest with Xu Heng (whom a reasonable juror could conclude was a co-conspirator) provides additional circumstantial evidence of the defendant’s intent and his knowledge and participation in the conspiratorial objective. The defendant arrived at the planned meeting location (one which he believed would be safe from the observation of Employee 1’s colleagues) with Xu Heng, travelled together under falsified visas (which a reasonable juror could conclude involved the help of additional co-conspirators). (*See* Gov. Ex. 11b). Xu Heng carried

the defendant's passport, along with \$7000 in U.S. currency, and a backpack full of equipment used to read, copy, and store large amounts of data. The defendant and Xu Heng carried four phones between them, one of which was wiped remotely after Xu Heng was arrested with the defendant.

In sum, the circumstantial evidence that the defendant entered into a criminal conspiracy is overwhelming. The defendant's contention to the contrary – which invites the Court to impermissibly weigh the evidence and assess the credibility of witnesses – should be rejected.

2. There is sufficient evidence for a reasonable juror to find the defendant intended to steal trade secrets with respect to Counts III and IV.

The defendant next argues that there is insufficient evidence for a reasonable juror to conclude that the defendant intended to steal trade secrets with respect to Counts III and IV, which specifically involve GE Aviation.

The record is clear that GE Aviation spent decades and hundreds of millions of dollars researching and developing the trade secrets used in the manufacture composite fan blade and containment system technology and took reasonable measures to protect these trade secrets, such as physical and cyber security. The evidence is also clear that the defendant attempted to illicitly obtain this secret information from GE Aviation, knowing that the information was protected. (Ex. 67c, p. 34 (“Is it possible to dump it to a portable hard drive or USB drive from work computer in advance?”) and page 36 (“Since there's still time, download more data and bring them. Anything design related will would work.”).)

Much of the same evidence highlighted above, provides sufficient evidence from which a jury could infer the defendant's intent. In addition to the above-described attempts by the defendant to entice GE Employee 1 to bring the contents of the GE Aviation hard drive and the tasking sheet which called for answers which would have been trade secrets, the government also

produced additional circumstantial evidence of the defendant's guilty intent: his overwhelmingly suspicious behavior. The defendant's use of an alias and multiple cover jobs to hide the fact that he worked as an intelligence officer of the MSS/JSSD—not to mention his direct involvement in the hacking of an aviation employee's computer—simply do not jibe with the argument that the defendant was merely seeking open source information. One does not need a fake name or fake job or the use of a sophisticated remote access trojan and compromised company employees to install that malware to read scientific journals, conduct internet searches, or network with academics or experts in the field. Indeed, a rational juror could reasonably conclude, that these are the actions of a spy intent on stealing what is not publicly available: valuable trade secrets.

The defendant's arguments to the contrary are unavailing and unpersuasive. In addition to ignoring the statutory definition of "trade secret," which includes technical, design, testing, other forms of information, the defendant focuses this Court on a strained reading of a few pieces of evidence in isolation, while excluding other highly relevant evidence.² And, again, the defendant asks this Court to do what it cannot – weigh the evidence.

Conclusion

In sum, there is sufficient evidence, when viewed in the light most favorable to the government, for a reasonable juror to find the government proved beyond a reasonable doubt that the defendant is guilty of all four counts in the indictment. As a result, the defendant's motion should be denied.

² For example, the defendant points to a statement in Exhibit 67c on p.9, where he states, "Teacher, as for now, there's nothing you need to prepare from my end." But the defendant ignores his statement on two days before (p. 8: "I'll touch base with the scientific research department to see what technology is desired and I will let you know what to prepare") and subsequent statements where he sought answers to the domestic requirements, the directory list, and the downloading of the computer.

Respectfully submitted,

VIPAL J. PATEL
Acting United States Attorney

s/Timothy S. Mangan
TIMOTHY S. MANGAN (0069287)
EMILY GLATFELTER
Assistant United States Attorney
221 East Fourth Street, Suite 400
Cincinnati, Ohio 45202
Office: (513) 684-3711
E-mail: timothy.mangan@usdoj.gov

MATTHEW J. MCKENZIE
Trial Attorney
National Security Division
Department of Justice
950 Pennsylvania Ave, NW
Washington, DC 20530
Office: (202) 514-7845
Email: matthew.mckenzie@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing has been electronically served via electronic mail upon defense counsel, this 2nd day of November, 2021.

s/Timothy S. Mangan

TIMOTHY S. MANGAN (0069287)
Assistant United States Attorney